

Response to Second Office Action
Docket No. 002.0132.US.UTL

Amendments to the Claims

This listing of claims will replace all prior versions, and listings, of claims in the application:

Listing of Claims:

- 1 1. (previously presented): A system for dynamically detecting
2 computer viruses through associative behavioral analysis of runtime state,
3 comprising:
4 a parameter set stored on a client system defining a group of monitored
5 events, each monitored event comprising a set of one or more actions defined
6 within an object, each action being performed by one or more applications
7 executing within a defined computing environment;
8 a monitor executing on the client system, comprising:
9 a collector continuously monitoring runtime state within the
10 defined computing environment for an occurrence of any one of the monitored
11 events in the group and tracking a sequence of execution of the monitored events
12 for each of the applications; and
13 an analyzer identifying each occurrence of a specific event
14 sequence characteristic of behavior of a computer virus and the application which
15 performed the specific event sequence, creating a histogram describing the
16 specific event sequence occurrence for each of the applications, and identifying
17 repetitions of the histogram associated with at least one object.
- 1 2. (original): A system according to Claim 1, further comprising:
2 a storage manager organizing the histograms into plurality of records
3 ordered by object, application, and monitored event.
- 1 3. (original): A system according to Claim 2, further comprising:
2 a structured databasc in which the plurality of records is stored; and

Response to Second Office Action
Docket No. 002.0132.US.UTL

3 the storage manager storing each histogram for each such specific event
4 sequence occurrence in one such database record identified by the application by
5 which the specific event sequence was performed.

1 4. (original): A system according to Claim 3, further comprising:
2 the storage manager configuring the structured database as an event log
3 organized by each event in the group of monitored events and updating the
4 database record storing each specific event sequence occurrence with a revised
5 histogram as each such occurrence is identified.

1 5. (original): A system according to Claim 1, further comprising:
2 the analyzer detecting suspect activities within each histogram, each
3 suspect activity comprising a set of known actions comprising a computer virus
4 signature.

1 6. (previously presented): A system according to Claim 5, wherein
2 each such suspect activity is selected from a class of actions comprising file
3 accesses, program executions, message transmissions, configuration area
4 accesses, security setting accesses, and impersonations.

1 7. (currently amended): A system according to Claim ~~[[6]]~~ 5, wherein
2 each such suspect activity is selected from a group comprising files accesses,
3 program executions, direct disk accesses, media formatting operations, sending of
4 electronic mail, system configuration area accesses, changes to security settings,
5 impersonations, and system calls having the ability to monitor system
6 input/output activities.

1 8. (previously presented): A system according to Claim 1, wherein
2 the computer virus comprises at least one form of unauthorized content selected
3 from a group comprising a computer virus application, a Trojan horse application,
4 and a hoax application.

Response to Second Office Action
Docket No. 002.0132.US.UTL

1 9. (previously presented): A method for dynamically detecting
2 computer viruses through associative behavioral analysis of runtime state,
3 comprising:
4 defining a group of monitored events, each monitored event comprising a
5 set of one or more actions defined within an object, each action being performed
6 by one or more applications executing within a defined computing environment;
7 continuously monitoring runtime state within the defined computing
8 environment for an occurrence of any one of the monitored events in the group;
9 tracking a sequence of execution of the monitored events for each of the
10 applications;
11 identifying each occurrence of a specific event sequence characteristic of
12 behavior of a computer virus and the application which performed the specific
13 event sequence;
14 creating a histogram describing the specific event sequence occurrence for
15 each of the applications; and
16 identifying repetitions of the histogram associated with at least one object.

1 10. (original): A method according to Claim 9, further comprising:
2 organizing the histograms into plurality of records ordered by object,
3 application, and monitored event.

1 11. (original): A method according to Claim 10, further comprising:
2 maintaining a structured database in which the plurality of records is
3 stored; and
4 storing each histogram for each such specific event sequence occurrence
5 in one such database record identified by the application by which the specific
6 event sequence was performed.

1 12. (original): A method according to Claim 11, further comprising:
2 configuring the structured database as an event log organized by each
3 event in the group of monitored events; and

Response to Second Office Action
Docket No. 002.0132.US.UTL

4 updating the database record storing each specific event sequence
5 occurrence with a revised histogram as each such occurrence is identified.

1 13. (original): A method according to Claim 9, further comprising:
2 detecting suspect activities within each histogram, each suspect activity
3 comprising a set of known actions comprising a computer virus signature.

1 14. (previously presented): A method according to Claim 13, wherein
2 each such suspect activity is selected from a class of actions comprising file
3 accesses, program executions, message transmissions, configuration area
4 accesses, security setting accesses, and impersonations.

1 15. (previously presented): A method according to Claim 13, wherein
2 each such suspect activity is selected from a group comprising files accesses,
3 program executions, direct disk accesses, media formatting operations, sending of
4 electronic mail, system configuration area accesses, changes to security settings,
5 impersonations, and system calls having the ability to monitor system
6 input/output activities.

1 16. (previously presented): A method according to Claim 9, wherein
2 the computer virus comprises at least one form of unauthorized content selected
3 from a group comprising a computer virus application, a Trojan horse application,
4 and a hoax application.

1 17. (previously presented): A computer-readable storage medium
2 holding code for dynamically detecting computer viruses through associative
3 behavioral analysis of runtime state, comprising:
4 defining a group of monitored events, each monitored event comprising a
5 set of one or more actions defined within an object, each action being performed
6 by one or more applications executing within a defined computing environment;
7 continuously monitoring runtime state within the defined computing
8 environment for an occurrence of any one of the monitored events in the group;

Response to Second Office Action
Docket No. 002.0132.US.UTL

9 tracking a sequence of execution of the monitored events for each of the
10 applications;
11 identifying each occurrence of a specific event sequence characteristic of
12 behavior of a computer virus and the application which performed the specific
13 event sequence;
14 creating a histogram describing the specific event sequence occurrence for
15 each of the applications; and
16 identifying repetitions of the histogram associated with at least one object.

1 18. (original): A storage medium according to Claim 17, further
2 comprising:
3 organizing the histograms into plurality of records ordered by object,
4 application, and monitored event.

1 19. (original): A storage medium according to Claim 18, further
2 comprising:
3 maintaining a structured database in which the plurality of records is
4 stored; and
5 storing each histogram for each such specific event sequence occurrence
6 in one such database record identified by the application by which the specific
7 event sequence was performed.

1 20. (original): A storage medium according to Claim 19, further
2 comprising:
3 configuring the structured database as an event log organized by each
4 event in the group of monitored events; and
5 updating the database record storing each specific event sequence
6 occurrence with a revised histogram as each such occurrence is identified.

1 21. (original): A storage medium according to Claim 17, further
2 comprising:

**Response to Second Office Action
Docket No. 002.0132.US.UTL**

- 3 detecting suspect activities within each histogram, each suspect activity
- 4 comprising a set of known actions comprising a computer virus signature.